4-23-2009

Twenty-First Century War Games

University of Dayton, Ohio (url: http://www.udayton.edu/index.php)

Twenty-First Century War Games

04.23.2009 | Culture and Society *Op-Ed pieces reflect the opinions of the authors and are not official University of Dayton positions.)*

The 1983 movie *War Games* featured a teen-age hacker who almost sets off "global thermonuclear war." Today, the technology in the movie seems hopelessly outdated as global nuclear holocaust has been replaced by terrorists with "dirty bombs."

What many of us don't realize is that the move's ultimate message is still valid: In War Games, the computer was the trigger that could set off weapons; today, computers are weapons.

This week, Defense Secretary Robert Gates told CBS News that the United States is "under cyberattack virtually all the time, every day" and that the Defense Department plans to more than quadruple the number of cyber experts it employs to ward off such attacks.

In 2007, Estonia was the target of a massive cyberattack that lasted two weeks. The attackers used Distributed Denial of Service (DDoS) attacks — targeting computers with too much traffic so they shut down.

The Estonian DDoS attack shut down computers used by government, media, businesses and schools. The attackers used a botnet — a network of 1 million "zombie" computers. Zombies are computers that belong to people like you and me; they've been taken over by software that lets an attacker use them in DDoS attacks. Since only part of the computer's resources are used, we never know our computer is moonlighting as an attack droid.

The Estonians knew the country was under attack. But by whom and why? It had to be crime or war (since terrorism is a type of crime). Individuals commit crime; countries commit war. It used to be easy to tell which was which: When Japan bombed Pearl Harbor, it was clear this was war, not crime.

It's not easy anymore. Estonia thought Russia was behind the attack, which made it war. It asked NATO to help, but NATO wasn't sure if this was war. The attack finally ended, and Estonia decided it was a crime — just retaliation by hackers who thought the country had insulted Russia.

Modern hackers don't have to hack NORAD to start a war; they can do it on their own, which creates a dilemma.

If a country doesn't know what an attack is, it doesn't know who responds. In the U.S., we divide response authority between the military (war) and law enforcement (crime). If we're hit with a cyberattack, who responds? It might come from another country, but that no longer means it's war. It might be war, or crime, or someone trying to trick us into believing another country is attacking us so we launch a counterattack.

Cyberspace blurs the lines between crime and war and that creates opportunities for the "bad guys." We must move beyond the notion of threats as "inside" (crime) or "outside" (war) and develop more flexible threat categories and more nuanced response systems. Here are some suggestions:

- Attacks often target civilians, who don't report them to authorities. The less we know about attacks and attackers, the harder it is to respond effectively.
- Integrate civilians into the response effort by encouraging them to report attacks and harden their systems to improve our ability to resist certain types of attacks.
- Integrate civilians, law enforcement and the military into an initiative that ensures the rapid flow of threat data across all three sectors. Incorporate procedures to preserve the operational distinction between law enforcement and military.
- Create a Cyber Security Agency to implement these efforts and serve as a conduit — within constitutionally permissible grounds -- between the military and law enforcement. The CSA should encourage and coordinate with similar efforts in other countries.

- Do NOT incorporate civilians into the response process itself. That creates possibilities for abuse, error and over-reaching.

Twenty-first-century hackers aren't bored adolescents. They're professionals: criminals, mercenaries and cyberwarriors. We're their targets. If we want to avoid becoming their victims, we must take cyberthreats seriously.